

New Constant-Weight Codes from Propagation Rules

Yeow Meng Chee, *Senior Member, IEEE*, Chaoping Xing and Sze Ling Yeo

Abstract—This paper proposes some simple propagation rules which give rise to new binary constant-weight codes.

Index Terms—constant-weight codes, cosets, q -ary codes

I. INTRODUCTION

THE ring $\mathbb{Z}/q\mathbb{Z}$ is denoted \mathbb{Z}_q . We endow \mathbb{Z}_q^n with the Hamming distance metric Δ : for $u, v \in \mathbb{Z}_q^n$, $\Delta(u, v)$ is the number of positions where u and v differ. A $(q$ -ary) code of length n is a subset $\mathcal{C} \subseteq \mathbb{Z}_q^n$. The elements of \mathcal{C} are called *codewords*, and the *size* of \mathcal{C} is the number of codewords it contains. The *minimum distance* of a code \mathcal{C} is $\Delta(\mathcal{C}) = \min_{u, v \in \mathcal{C}, u \neq v} \Delta(u, v)$. We often denote by $(n, d)_q$ -code a q -ary code of length n and minimum distance at least d .

The *weight*, $\text{wt}(u)$, of $u \in \mathbb{Z}_q^n$ is its distance from the origin, that is, $\text{wt}(u) = \Delta(u, 0)$. For $0 \leq w \leq n$, the $(q$ -ary) *Johnson space* $J_q^n(w)$ is the set of all elements of \mathbb{Z}_q^n having weight w , that is, $J_q^n(w) = \{u \in \mathbb{Z}_q^n : \text{wt}(u) = w\}$. A $(q$ -ary) *constant-weight code* of length n , distance d , and weight w , denoted $(n, d, w)_q$ -code, is a code $\mathcal{C} \subseteq J_q^n(w)$ such that $\Delta(\mathcal{C}) \geq d$.

We adopt the convention throughout this paper that if q is not specified, then we assume $q = 2$. Hence, for example, an (n, d, w) -code refers to an $(n, d, w)_2$ -code, and $J^n(w)$ refers to $J_2^n(w)$.

Binary constant-weight codes have been extensively studied for more than four decades due to their fascinating combinatorial structures and applications [1]–[19]. Given n , d , and w , the central problem of interest in binary constant-weight codes is in the determination of $A(n, d, w)$, the largest possible size of an (n, d, w) -code. Exact values of $A(n, d, w)$ are known only for a few infinite families of parameters n , d , and w , and in some other sporadic instances (see, for example, [3], [4]). In light of the difficulty of determining $A(n, d, w)$ exactly, various bounds have also been developed. There are two online tables devoted to bounds on $A(n, d, w)$: one maintained by Rain and Sloane [20] and the other by Smith and Montemanni [21]. While the former table considers codes of lengths not

exceeding 63, the latter table focuses mainly on codes for lengths between 29 and 63, having small weights.

In this paper, we present simple propagation rules for binary constant-weight codes through q -ary codes. It turns out that some good binary constant-weight codes can be obtained from these propagation rules. In particular, we improve on a number of bounds in the online tables of Rain and Sloane [20], and Smith and Montemanni [21].

We remark that the table of Smith and Montemanni [21] was created because the table of Rains and Sloane [20] had not been updated for many years. For code parameters that are not covered by Smith and Montemanni [21], we have checked against recent literature, to the best of our efforts, in ascertaining that our results here do indeed improve upon existing results.

II. PROPAGATION RULES

In this section, we present some simple propagation rules for binary constant-weight codes from q -ary codes. We begin with a simple observation.

Let $\mathcal{C} \subseteq \mathbb{Z}_q^n$. For $u \in \mathbb{Z}_q^n$, we denote by $u + \mathcal{C}$ the *coset* of \mathcal{C} ,

$$\{u + c : c \in \mathcal{C}\}.$$

We also embed \mathbb{Z}_2 into \mathbb{Z}_q . It is evident that $(u + \mathcal{C}) \cap J^n(w)$ is a binary constant-weight code of weight w and size $N = |(u + \mathcal{C}) \cap J^n(w)|$. Since the minimum distance d' of $(u + \mathcal{C}) \cap J^n(w)$ is at least d and d' must be even, it follows that $d' \geq 2\lfloor(d+1)/2\rfloor$. Thus, we have the following.

Theorem 2.1: Let $0 < w < n$. If there exists an $(n, d)_q$ -code \mathcal{C} , then there exists an $(n, 2\lfloor(d+1)/2\rfloor, w)$ -code of size N , where

$$N = \max_{u \in \mathbb{Z}_q^n} |(u + \mathcal{C}) \cap J^n(w)|.$$

A simple bound on the size of the constant-weight codes in Theorem 2.1 can be obtained by considering the average size of the cosets.

Theorem 2.2: Let $0 < w < n$. If there exists an $(n, d)_q$ -code of size M , then

$$A(n, 2\lfloor(d+1)/2\rfloor, w) \geq \left\lceil \frac{M \binom{n}{w}}{q^n} \right\rceil.$$

Proof: Let \mathcal{C} be an $(n, d)_q$ -code of size M . Let u_1, u_2, \dots, u_{q^n} denote all the elements of \mathbb{Z}_q^n , and let

The research of Y. M. Chee is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040. The research of C. Xing is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T208B2206.

Y. M. Chee, C. Xing and S. L. Yeo are with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371 (email: ymchee@ntu.edu.sg, xingcp@ntu.edu.sg, yeos1@ntu.edu.sg).

Corresponding author: C. Xing.

$v_1, v_2, \dots, v_{\binom{n}{w}}$ denote all the elements of $J^n(w)$. Define

$$\delta_{i,j} = \begin{cases} 1, & \text{if } v_j \in u_i + \mathcal{C} \\ 0, & \text{if } v_j \notin u_i + \mathcal{C}. \end{cases}$$

For each $v_j \in J^n(w)$, there are M elements $u_i \in \mathbb{Z}_q^n$ such that $u_i + \mathcal{C}$ contains v_j (to see this, note that $v_j \in u_i + \mathcal{C}$ if and only if $u_i = v_j + c$ for some $c \in \mathcal{C}$). Thus,

$$\sum_{1 \leq i \leq q^n} \sum_{1 \leq j \leq \binom{n}{w}} \delta_{i,j} = M \binom{n}{w}.$$

Hence, there exists at least one ℓ , $1 \leq \ell \leq q^n$, such that

$$\sum_{1 \leq j \leq \binom{n}{w}} \delta_{\ell,j} \geq \frac{M \binom{n}{w}}{q^n}.$$

The theorem now follows by noting that the size of $(u_\ell + \mathcal{C}) \cap J^n(w)$ is precisely $\sum_{1 \leq j \leq \binom{n}{w}} \delta_{\ell,j}$, and we have seen above that $(u_\ell + \mathcal{C}) \cap J^n(w)$ is an $(n, 2\lfloor(d+1)/2\rfloor, w)$ -code. ■

Next, we consider binary constant-weight codes of length $n+1$ from q -ary codes of length n .

Theorem 2.3: Let $0 < w < n$. Suppose there exists an $(n, d)_q$ -code \mathcal{C} of size M . Then,

- (i) there exists an $(n+1, 2\lfloor(d+1)/2\rfloor, w)$ -code of size N , where

$$N = \max_{u \in \mathbb{Z}_q^n} |(u + \mathcal{C}) \cap (J^n(w-1) \cup J^n(w))|;$$

- (ii)

$$A(n+1, 2\lfloor(d+1)/2\rfloor, w) \geq \left\lceil \frac{M(\binom{n}{w-1} + \binom{n}{w})}{q^n} \right\rceil.$$

Proof:

- (i) Let $u \in \mathbb{Z}_q^n$ such that $|(u + \mathcal{C}) \cap (J^n(w-1) \cup J^n(w))|$ achieves the maximum size N . It is clear that $\mathcal{C}' = (u + \mathcal{C}) \cap (J^n(w-1) \cup J^n(w))$ is an (n, d) -code, where each codeword has weight either $w-1$ or w . To each codeword $c \in \mathcal{C}'$, append a new coordinate which takes on value one if $\text{wt}(c) = w-1$ and value zero if $\text{wt}(c) = w$. The set of resulting codewords is an $(n+1, 2\lfloor(d+1)/2\rfloor, w)$ -code.
- (ii) Using the same arguments as in the proof of Theorem 2.2, we get an (n, d) -code of size $M(\binom{n}{w-1} + \binom{n}{w})/q^n$, in which the weight of every codeword is either $w-1$ or w . By appending a new coordinate to every codeword as in (i) above, we get an $(n+1, 2\lfloor(d+1)/2\rfloor, w)$ -code of the required size. ■

III. EXAMPLES

We provide some examples where the propagation rules given by Theorems 2.2 and 2.3 lead to improved bounds on $A(n, d, w)$.

In the tables of this section, a bold entry indicates that the size of the code constructed here is larger than any known

codes of the same parameters, and a entry superscripted by an asterisk indicates that the size of the code constructed here is of the same size as the best known code of the same parameters. M_{\max} denotes the lower bound on $A(n, d, w)$ given by Theorems 2.1 or 2.3(i), and M_{avg} denotes the lower bound on $A(n, d, w)$ given by Theorems 2.2 or 2.3(ii). M_{RS} denotes the lower bound on $A(n, d, w)$ in the tables of Rains and Sloane [20].

Example 3.1: Let \mathcal{C} be the Goethals $(63, 7)$ -code of size 2^{47} [22] (see [23, Chapter 5] for the structure of this code).

- Theorems 2.2 and 2.3(ii) give

$$A(63, 8, w) \geq \left\lceil \binom{63}{w} / 2^{16} \right\rceil,$$

$$A(64, 8, w) \geq \left\lceil \left(\binom{63}{w-1} + \binom{63}{w} \right) / 2^{16} \right\rceil.$$

The implications of these bounds are given in Table I.

TABLE I
SOME CONSTANT-WEIGHT CODES OF DISTANCE EIGHT

Lower Bounds on $A(63, 8, w)$			Lower Bounds on $A(64, 8, w)$		
w	M_{avg}	M_{RS}	w	M_{avg}	M_{RS}
7	8443	7182	7	9480	8064
8	59096	50274	8	67538	57456
9	361141	-	9	420236	-
10	1950158	-	10	2311298	-
11	9396214	-	11	11346372	-
12	40716926	-	12	50113140	-
13	159735632	-	13	200452558	-
14	570484400	-	14	730220032	-

- Shortening \mathcal{C} at the last i positions, $1 \leq i \leq 46$, results in a $(63-i, 7)$ -code of size 2^{47-i} . It follows from Theorem 2.2 that there exists a $(63-i, 8, 7)$ -code of size $\binom{63-i}{7} / 2^{16}$. In particular, when $i \in \{1, 2, 3\}$, this implies

$$A(62, 8, 7) \geq 7505, \quad (1)$$

$$A(61, 8, 7) \geq 6657, \quad (2)$$

$$A(60, 8, 7) \geq 5894. \quad (3)$$

The three lower bounds (1)–(3) improve those in [21] (the corresponding lower bounds given there are 6693, 6223, and 5770, respectively, obtained by Smith et al. [13]).

Example 3.2: Let \mathcal{C} be the Preparata $(63, 5)$ -code of size 2^{52} [24] (see [23, Chapter 5] for the structure of this code). Theorems 2.2 and 2.3(ii) give

$$A(63, 6, w) \geq \left\lceil \binom{63}{w} / 2^{11} \right\rceil,$$

$$A(64, 6, w) \geq \left\lceil \left(\binom{63}{w-1} + \binom{63}{w} \right) / 2^{11} \right\rceil.$$

We also found via computation cosets of \mathcal{C} achieving the maximum in Theorems 2.1 and 2.3(i). The results are given in Tables II and III.

Example 3.3: Let \mathcal{C} be the (linear) $(31, 9)$ -code of size 2^{13} constructed by Grassl [25].

TABLE II
LOWER BOUNDS ON $A(63, 6, w)$

w	M_{avg}	M_{max}	M_{RS}
5	3433	3906*	3906
6	33177	37758*	37758
7	270152	270468	264771
8	1891062	1893276	1853397
9	11556490	11594310*	11594310
10	62405042	62609274*	62609274
11	300678837	300700062	300496392
12	1302941625	1302990507	1302151032
13	5111540218	5112164988*	5112164988
14	18255500778	18257732100*	18257732100

TABLE III
LOWER BOUNDS ON $A(64, 6, w)$

w	M_{avg}	M_{max}	M_{RS}
5	3723	3906	-
6	36609	41664*	41664
7	303329	303354	-
8	2161214	2163744	2118168
9	13447552	13447707	-
10	73961530	74203584*	74203584
11	363083878	363105666	-
12	1603620460	1603680624	1602647424
13	6414481842	6414487191	-
14	23367040996	23369897088*	23369897088

TABLE IV
SOME CONSTANT-WEIGHT CODES OF DISTANCE 10

Lower Bounds on $A(31, 10, w)$			Lower Bounds on $A(32, 10, w)$		
w	M_{max}	M_{RS}	w	M_{max}	M_{RS}
11	387	-	11	585	-
12	612	-	12	953	-
13	872	-	13	1443	-
14	1106	-	14	1923	-

- We found via computation cosets of \mathcal{C} achieving the maximum in Theorems 2.1 and 2.3(i). The results are given in Table IV.
- Shortening \mathcal{C} at the last two positions results in a (linear) (29, 9)-code of size 2^{11} . We found, via computation, cosets of this shortened code achieving the maximum in Theorem 2.3(i). This gives $A(30, 10, 12) \geq 390$. Lower bounds on $A(30, 10, 12)$ are previously not known.

Example 3.4: Let \mathcal{C} be the (linear) BCH (31, 11)-code of size 2^{11} [26], [27] (see [23, Chapter 8] for the structure of this code).

- We found, via computation, cosets of \mathcal{C} achieving the maximum in Theorems 2.1 and 2.3(i). The results are given in Table V.

TABLE V
SOME CONSTANT-WEIGHT CODES OF DISTANCE 12

Lower Bounds on $A(31, 12, w)$			Lower Bounds on $A(32, 12, w)$		
w	M_{max}	M_{RS}	w	M_{max}	M_{RS}
9	40	-	9	40	-
10	87	-	10	122	-
11	186	-	11	186	-
12	310	-	12	496	-
13	400	-	13	400	-
14	510	-	14	900	-

- Shortening \mathcal{C} at the last i positions, $i \in \{1, 2\}$, results in a $(31 - i, 11)$ -code of size 2^{11-i} . We found, via

computation, cosets of these shortened codes achieving the maximum in Theorems 2.1 and 2.3 (i). These provide the lower bounds

$$A(29, 12, 11) \geq 76,$$

$$A(29, 12, 12) \geq 114,$$

$$A(29, 12, 13) \geq 140,$$

and

$$A(30, 12, 10) \geq 66,$$

$$A(30, 12, 11) \geq 120,$$

$$A(30, 12, 12) \geq 190,$$

$$A(30, 12, 13) \geq 234,$$

$$A(30, 12, 14) \geq 288.$$

Previously, no lower bounds are known on $A(n, 12, w)$ for these parameter sets.

Example 3.5: Let \mathcal{C} be the (linear) (31, 13)-code of size 2^7 constructed by Grassl [25]. We found, via computation, cosets of \mathcal{C} achieving the maximum in Theorem 2.3(i). These provide the lower bounds

$$A(32, 14, 12) \geq 29,$$

$$A(32, 14, 13) \geq 42.$$

Lower bounds on $A(32, 14, w)$, $w \in \{12, 13\}$, are previously not known.

Example 3.6: Let \mathcal{C}_0 be the (linear) Reed-Muller (32, 16)-code of size 2^6 , and let \mathcal{C} be the code obtained from \mathcal{C}_0 by puncturing it at the last position. Then \mathcal{C} is a (31, 15)-code of size 2^6 . We found, via computation, cosets of \mathcal{C} achieving the maximum in Theorems 2.1 and 2.3(i). These provide the lower bounds

$$A(n, 16, 13) \geq 16,$$

$$A(n, 16, 14) \geq 21,$$

$$A(n, 16, 15) \geq 31,$$

for $n \in \{31, 32\}$. Lower bounds on $A(n, 16, w)$ are previously not known for these parameters.

ACKNOWLEDGMENT

The authors are grateful to Ding Yang and Chen Jie for their help on programming, to Xing Zhengrong for several discussions on Theorem 2.1, and to the anonymous reviewer for invaluable comments and suggestions.

REFERENCES

- [1] S. M. Johnson, "Upper bounds for constant weight error-correcting codes," *Discrete Math.*, vol. 3, pp. 109–124, 1972.
- [2] R. L. Graham and N. J. A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. 26, no. 1, pp. 37–43, 1980.
- [3] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory*, vol. 36, no. 6, pp. 1334–1380, 1990.
- [4] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2373–2395, 2000.

- [5] A. Barg, "Extremal problems of coding theory," in *Coding Theory and Cryptology (Singapore, 2001)*, ser. Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap. World Sci. Publ., River Edge, NJ, 2002, vol. 1, pp. 1–48.
- [6] H. K. Aw, Y. M. Chee, and A. C. H. Ling, "Six new constant weight binary codes," *Ars Combin.*, vol. 67, pp. 313–318, 2003.
- [7] Z. Zhong, D. Wang, Y. Cui, M. W. Bockrath, and C. M. Lieber, "Nanowire crossbar arrays as address decoders for integrated nanosystems," *Science*, vol. 302, pp. 1377–1379, 2003.
- [8] T. Etzion and M. Schwartz, "Perfect constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2156–2165, 2004.
- [9] S.-T. Xia, F.-W. Fu, Y. Jiang, and S. Ling, "The probability of undetected error for binary constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 9, pp. 3364–3373, 2005.
- [10] C. Xing and J. Ling, "A construction of binary constant-weight codes from algebraic curves over finite fields," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3674–3678, 2005.
- [11] L. Ji, "Asymptotic determination of the last packing number of quadruples," *Des. Codes Cryptogr.*, vol. 38, no. 1, pp. 83–95, 2006.
- [12] P. J. Kuekes, W. Robinett, R. M. Roth, G. Seroussi, S. S. Gregory, and R. S. Williams, "Resistor-logic demultiplexers for nanoelectronics based on constant-weight codes," *Nanotechnology*, vol. 17, pp. 1052–1061, 2006.
- [13] D. H. Smith, L. A. Hughes, and S. Perkins, "A new table of constant weight codes of length greater than 28," *Electron. J. Combin.*, vol. 13, no. 1, Article #A2, p. 18 (electronic), 2006.
- [14] S.-T. Xia, F.-W. Fu, and S. Ling, "A lower bound on the probability of undetected error for binary constant weight codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4235–4243, 2006.
- [15] Y. M. Chee, "A new lower bound for $A(17, 6, 6)$," *Ars Combin.*, vol. 83, pp. 361–363, 2007.
- [16] F.-W. Fu and S.-T. Xia, "The characterization of binary constant weight codes meeting the bound of Fu and Shen," *Des. Codes Cryptogr.*, vol. 43, no. 1, pp. 9–20, 2007.
- [17] I. Gashkov, J. A. O. Ekberg, and D. Taub, "A geometric approach to finding new lower bounds of $A(n, d, w)$," *Des. Codes Cryptogr.*, vol. 43, no. 2-3, pp. 85–91, 2007.
- [18] I. Gashkov and D. Taub, "New optimal constant weight codes," *Electron. J. Combin.*, vol. 14, no. 1, pp. Note 13, 6 pp. (electronic), 2007.
- [19] Y. M. Chee and A. C. H. Ling, "Limit on the addressability of fault-tolerant nanowire decoders," *IEEE Trans. Comput.*, vol. 58, no. 1, pp. 60–68, 2009.
- [20] E. M. Rains and N. J. A. Sloane, "Table of constant weight binary codes," URL=<http://www.research.att.com/~njas/codes/Andw/>.
- [21] D. H. Smith and R. Montemanni, "Bounds for constant weight binary codes with $n > 28$," URL=<http://www.idsia.ch/~roberto/Andw29/>.
- [22] J.-M. Goethals, "Two dual families of nonlinear binary codes," *Electron. Lett.*, vol. 10, pp. 471–472, 1974.
- [23] S. Ling and C. Xing, *Coding Theory - A First Course*. Cambridge: Cambridge University Press, 2004.
- [24] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Information and Control*, vol. 13, pp. 378–400, 1968.
- [25] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," URL=<http://www.codetables.de>.
- [26] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.
- [27] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, 1960.